

确保 IoT 设备安全需要转变思维

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Securing IoT Devices Requires a Change in Thinking		
原文作者	Dr.Phillip Hallam-Baker	原文发布日期	2017 年 5 月 15 日
作者简介	Dr.Phillip Hallam-Baker 是一家全球安全公司，科莫多的副董事长和首席科学家。 http://www.darkreading.com/author-bio.asp?author_id=3755		
原文发布单位	Dark reading		
原文出处	http://www.darkreading.com/iot/securing-iot-devices-requires-a-change-in-thinking/a/d-id/1328967?		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antivy.cn 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。 		

确保 IOT 设备安全需要转变思维

解决 IoT 设备安全问题没有灵丹妙药，只有检测、减缓的方法。

预测物联网（IoT）灾难就有点像是预测泰坦尼克的悲惨结局一样。我们以前都看过这个电影，知道电影的结局。

要了解 IoT 安全问题有多大，我们需要回到 20 世纪 70 年代，现在所谓的 Modbus 通信协议被引入和应用用于工业控制系统。

目前，同样的协议仍在使用，而且很多控制设备的运行代码仍未更改。任何一台连接 Modbus 链上的设备，都可以完全控制链上的每一台设备。最近，在一次 IoT 安全会议上，发言人强调需要获得 IoT 固件不断更新的能力作为核心安全原则。然而，制造商过去 30 多年为什么没有看到更新核心的关键点呢？

坚持沿用过去的方法控制世界，是因为其它方法更糟。化工行业，最重要的两个问题是安全和保持工厂的运行。但它们往往是同一问题，一台机器可能突然自动脱机 10 分钟，因为安装时制造商认为“重要的安全更新”可能会使整个工厂停工一天或更长时间。如果一个熔炉出现了问题，这可能会使一个有价值的工艺流程转变成花费巨力处理工业废物。

一些减少 IoT 安全问题的方法

行业从桌面和服务器上消除的安全漏洞再次出现在应用层。而现在他们正在重建物联网世界。解决物联网安全没有灵丹妙药，但有一些检测和减轻问题的方法。

- 最少特权：机器，进程或用户能操作的越少，造成损害的机会就越少。如果无法把损失减少到最低限度，隔离 IoT 设备和代码使得攻击面可控。

- 最简洁：软件系统越复杂，越难测试，越有可能出现错误。基于简单设备模式，工业控制系统连接到系统中心，在系统中心限制设备的复杂度。

- 审查：另一个强大的工具是审查。物联网设备的反社会习惯是意想不到的，通常未公开尝试与外界通信。这给具有应用防火墙服务产品的公司带来了困境。

当然，明智、有安全意识的首席信息安全官员可能会宣布暂停使用 IoT 设备，直到行业自行排除并开始提供可预测的可靠和安全的产品。

前路何在？

检测和减缓措施仍是目前和以后的必备措施，但成本高昂。设备的攻击面越多，管理成本越高。诸如 Windows 和 Linux 等操作系统因为其灵活的功能，这为对手提供了很大的攻击面。因此，即使是 Linux 内核包含 1590 万行代码（v3.6）。几乎所有的代码都是用 C 或 C++编写的，因此容易受到缓冲区溢出攻击。

目前，我们处于 IoT 设备最脆弱的时期。五年前，大多数嵌入式系统控制器都是围绕 8 位或 16 位 CPU 构建的，很少提供超过几千字节的 RAM。今天，一个 32 位 CPU，内存几千兆字节，只需要几分钱。IoT 设备推向市场的最便宜，最快捷的方法是将完整的 Linux 发行版放到芯片上，并将其用作开发系统。要提高物联网安全性，需要做两件事情：

- 必须开发一种度量尺度，允许 IoT 设备购买者估计可能出现的攻击面。
- 制造商必须相信，当他们做出购买决定时，这个度量尺度对他们的客户重要。

今天，大多数 IoT 设备的 99% 的代码复杂度来自于它围绕的操作系统核心。而不是将 IoT 设备的软件作为在桌面操作系统上运行的应用程序，而是从更小的东西开始。我们应该从尽可能的简化事情，尽量不添加，而不是使用一些非常复杂，需要移除功能的东西。